VPN

General description

A virtual private network is a computer network, that is established over a different kind of communications channel (usually over the internet), but does not work as if it were part of it. The three main aspects about it are:

- It is a network connection to a computer, that is not reachable otherwise, or should not be contacted without the VPN connection (*network*).
- The communication is encrypted, so that the communications content cannot be monitored (*private*).
- It is not a physical connection like a LAN connection via wires. However, of course, some sort of physical connection is required. It is not really important, how the data transport is achieved. From inside the VPN it looks like a physical connection to the other peers in the VPN, much like a physical LAN connection, but it is not (necessarily) one. It may be carried by any combination of outside carrier techniques (*virtual*).

Applications

There are in principle two main goals you can achieve using a VPN:

1. A connection over a not secure channel, secured from prying eyes by the VPN encryption. This is especially important, if you have really sensitive data to transport (e. g. using an otherwise not encrypted channel, like http protocol without SSL/TLS), but the outside infrastructure may be compromised (e. g. unencrypted wireless LAN).
2. The other main application is establishing a connection at all, that might not be possible over the internet. A common reason are programs, that only work on their own subnet, e. g. LAN servers. Another examples may be protocols or services, that should not be visible via internet but contactable by the means of using an internet connection.

Of course there is also the possibility of combining the former two reasons into one. E. g., have the computer of an employee *never* connect to the internet directly, but only via VPN through the company's (secured) network. In this case, the only allowed connection via the internet is the actual VPN tunnel. From the company's network you may connect to the rest of the internet via a firewall or other suitably secured internet connection.

Gaming

In the gaming community, the security aspect is mostly negligible. Usually the reasons for using a VPN are one of the two: Either you simply cannot connect to a server over the internet (e. g. running game servers only accepting connections from the local subnet) or you don't want the server to appear online (purposely running a LAN server, which can only be connected/seen by friends via the VPN).

Security Considerations

There are people concerned about the security aspects of VPN solutions, especially the free ones. Here are a few words about VPN and gaming in general. When using a VPN solution, make sure you can trust everybody on the same network, that is able to connect to your computer, make sure they cannot do any damage:

1. When in doubt, be sure to have no services running, that might compromise security. That goes especially for unprotected SMB shares, FTP servers or running the computer without any firewall (and no, the Windows firewall is only a starter kit, not a bullet-proof solution). So essentially, basic computer network security should always be an issue, but especially when using a VPN with people you do know nothing about.
2. If a VPN solution is known to use weak encryption, don't use it! It is basically like connecting your computer directly to the internet. Once an encryption of a VPN is broken, an attacker may break into the VPN connection at will and do any kind of things just like working from within your LAN. Even a simple NAT router would provide more security protection than that.

[Games Database] [Network Terms]